

AFFIDAVIT OF SPECIAL AGENT BRIAN PEREIRA

I, Brian Pereira, declare and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) for approximately 15 years. I am currently assigned to the Lakeville Resident Agency within the Boston Division, where my primary duties involve the investigation of a wide variety of federal criminal offenses.

2. I graduated from the FBI Academy in April 2008 and was assigned to the FBI New York, Criminal Division, until October 2014 investigating Transnational Organized Crime matters. I was then assigned to the FBI Boston, Organized Crime Drug Enforcement Task Force (“OCDETF”) Boston Strike Force, which is a joint task force incorporating various law enforcement agencies, including the FBI, the Drug Enforcement Administration (“DEA”), Homeland Security Investigations (“HSI”), and the U.S. Marshals Service (“USMS”), among other agencies. Currently, I am assigned to the Lakeville Resident Agency within the Boston Division where my primary duties involve the investigation of a wide variety of federal criminal offenses, including those related to complex financial crimes.

PURPOSE OF THE AFFIDAVIT

3. I submit this affidavit in support of a Verified Complaint for Forfeiture *in Rem* against the following assets:

- a. 0.0066488 BTC seized from BINANCE account with user ID XXXX0976 and the wallet address of 1BqNAXgppfFTFRTXtiU6FebqR1XDzyNjYN (“BINANCE ACCOUNT 0976”) on or about August 22, 2022;
- b. 0.02426 BTC seized from BINANCE account with user ID XXXXX0823 (“BINANCE ACCOUNT 0823”) and the wallet address of 1JTew9xoybR1RGvhtY9pTP4uLdND8smgzE on or about August 22, 2022;

- c. 736.652108 USDT seized from BINANCE account with user ID XXXX5423 (“BINANCE ACCOUNT 5423”) and the wallet address of 1EVBUg9v14xVwySnQeWKLP75suYwxK99zF on or about August 23, 2022;
- d. 19512.815843 USDT, 27.58652 APE, 10292.6775 JASMY, 648.193 OGN, 18906045.54 SHIB seized from BINANCE account with user ID XXXX5607 (“BINANCE ACCOUNT 5607”) and the wallet address of 1GRo1bpNQnHLGrqhkasyGYzydNcyNgbGV on or about August 23, 2022;
- e. 5113150.55 XEC seized from BINANCE ACCOUNT 5607 on or about September 19, 2022;
- f. 1577.9271 USDT and 19240.7898 TLM seized from BINANCE account with user ID XXXX9975 (“BINANCE ACCOUNT 9975”) and the wallet address of 1LGvW7BTgTxUWPQqLQYsygcSLPXahrMMM5 on or about August 23, 2022;
- g. 0.00217033 BTC and .01266977 BNB seized from BINANCE account with user ID XXXX5323 (“BINANCE ACCOUNT 5323”) and the wallet address of 169QRmoJP6SFmDW2SqWjVHd2RdmzbBiNda on or about August 22, 2022; and
- h. 2875.828369 USDT seized from BINANCE account with user ID XXXX2809 (“BINANCE ACCOUNT 2809”) and the wallet address of 1P6fDHjCNkkAsVqrXpFraGG13DfuGh6Mhm on or about August 23, 2022

(collectively, the “Defendant Cryptocurrency” and the “BINANCE ACCOUNTS”).¹

4. As set forth below, there is probable cause to believe that the Defendant Cryptocurrency is traceable to and/or involved in a sophisticated business email compromise (“BEC”) fraud scheme which targeted a law firm located on Cape Cod, Massachusetts. The scheme duped principals of the firm into completing an improperly routed bank wire transfer of \$898,342.27 from one of the firm’s Massachusetts-based bank accounts. The investigation has determined that portions of the law firm’s \$898,342.27 in misdirected funds were ultimately transferred into the BINANCE ACCOUNTS.

¹ BTC (bitcoin), USDT (Tether), APE (APEcoin), JASMY (an Ethereum token), OGN (Origin Protocol), SHIB (Shiba Inu), XEC (eCash), TLM, and BNB (Binance coin) are all forms of cryptocurrency.

5. Accordingly, there is probable cause to believe that the Defendant Cryptocurrency is property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud) and § 1349 (wire fraud conspiracy), and therefore are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). There is also probable cause to believe that the BINANCE ACCOUNTS and the Defendant Cryptocurrency is property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (money laundering), or are traceable to such property, and therefore are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A). The Defendant Cryptocurrency was seized pursuant to seizure warrants issued in the District of Massachusetts.

6. The statements contained in this affidavit are based upon written reports about this investigation that I have received, directly or indirectly, from other law enforcement agents, officers, and other witnesses; information gathered from the service of subpoenas and records requests; independent investigation and analysis by FBI agents and analysts; and my own investigation and experience, training, and background as a Special Agent with the FBI.

7. Because this affidavit is being submitted for the limited purpose of showing probable cause, I have not included each and every fact known to me and other law enforcement officers involved in this investigation. Rather, I have included only those facts that I believe are necessary to establish probable cause for the issuance of the requested seizure warrants.

FORFEITURE AUTHORITY

8. Under 18 U.S.C. § 981(a)(1)(C), property, real or personal, which constitutes or are derived from proceeds traceable to a violation of a specified unlawful activity or conspiracy to commit such offense, specifically violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (wire fraud conspiracy), is subject to civil forfeiture. Pursuant to 18 U.S.C. § 1961(1), as

incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity.

9. Under 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. § 1956], or any property traceable to such property” is subject to forfeiture to the United States. The First Circuit has found that the term “property involved” means both tainted and untainted property which have been comingled, so long as the “comingling was done to facilitate money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(i).” *U.S. v. McGauley*, 279 F.3d 62, 76 (1st Cir. 2002); *see also U.S. v. Lyons*, 870 F. Supp. 2d 281, 285-86 (D. Mass. 2012).

10. Pursuant to 18 U.S.C. § 1956(a)(1)(B)(i), a person commits the crime of money laundering when “knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity” and does so knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity....” Pursuant to 18 U.S.C. § 1956(h), it is also a crime to conspire to commit money laundering.

BACKGROUND ON CRYPTOCURRENCY

11. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (“BTC”), Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually

stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.² Cryptocurrency is not illegal in the United States.

12. Bitcoin³ is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (*i.e.*, online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the

² Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

³ Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it is not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

13. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

14. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, including money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency

for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces.

15. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g., Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code⁴ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

⁴ A QR code is a matrix barcode that is a machine-readable optical label.

16. Bitcoin “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁵ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act (“BSA”) anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

⁵ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

17. Some companies offer cryptocurrency wallet services, which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

18. Binance is a cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets.

PROBABLE CAUSE

The Scheme to Defraud

19. In March 2022, a representative from an Orleans, Massachusetts law firm, contacted the FBI to report that the law firm fell victim to a BEC scheme. The law firm reported it was tricked into wiring \$898,342.27 from one of the firm's Massachusetts bank accounts to a Bank of America ("BOA") account number, XXXXXXXX1213 ("BOA Account 1).

20. The law firm sent the \$898,342.27 wire on or about March 15, 2022 after two firm employees received an email containing the fraudulent wire instructions that appeared to come from a trusted business associate.⁶ Specifically, the fraudulent instructions originated from an email address closely resembling the trusted business associate's actual email address, differing by one letter.

21. Bank records indicate BOA Account 1—the account to which the firm was tricked into sending funds—was opened on February 4, 2022 at a BOA branch located in California. The accountholder and only authorized signer is an individual that the law firm does not know and with whom they have no business relationship.

The Subsequent Transfer of Funds, Conversion to Cryptocurrency, and Money Laundering

22. BOA records reveal that following receipt of the law firm's misdirected wire into BOA Account 1, substantially all of the fraud proceeds⁷ were almost immediately transferred into a second BOA account numbered XXXXXXXX7023 ("BOA Account 2"), which was also maintained by the individual who controlled BOA Account 1, and appears to have been opened at the same time as BOA Account 1.

23. BOA records further reveal that almost immediately following transfer of the

⁶ The investigation determined that the fraudulent email is associated with a website domain maintained by namecheap.com which is well-known, US based budget web-hosting provider.

Records obtained from namecheap.com reveal that the domain name was created on March 14, 2022 (the day before the fraudulent wire was initiated). The person who appears as the customer is not associated with the address provided, which is a single-family home located in a residential neighborhood of Queens, New York.

⁷ Within days of receipt of the \$898,342.27 in funds into BOA Account 1, substantially all of the funds were transferred into BOA Account 2, as follows: Transfer 1, 3/15 \$780,000, Transfer 2, 3/17 \$113,261.95, Transfer 3, 3/18 \$3,000, Transfer 4, 3/18 \$1,500, Transfer 5, 3/21 \$500. (The total of Transfers 1 through 5 is \$898,261.95.)

stolen funds to BOA Account 2, there were four, large outgoing transfers from BOA Account 2 to an account at Gemini Trust Company, a cryptocurrency exchange (“Gemini”) (“Gemini Account 1”), maintained by the same person as the two BOA accounts. The outgoing transfers—for \$751,000, \$136,342 and \$6,000, and \$5,000—totaling \$898,342—were completed during the period from March 16, 2022 through March 21, 2022.⁸

24. Once the \$898,342 arrived in Gemini Account 1, the funds were converted to BTC and withdrawn to three different BTC addresses:

bc1qmnene7eer2nhmds0wag9hnydrdcna7k9vukcr,

bc1qnv32zm7caegv93mfvyk9tke5hdzmqp2vdsn67, and

bc1qz3jvprynp9w753wsuxnuskqt287etxa9uda754.

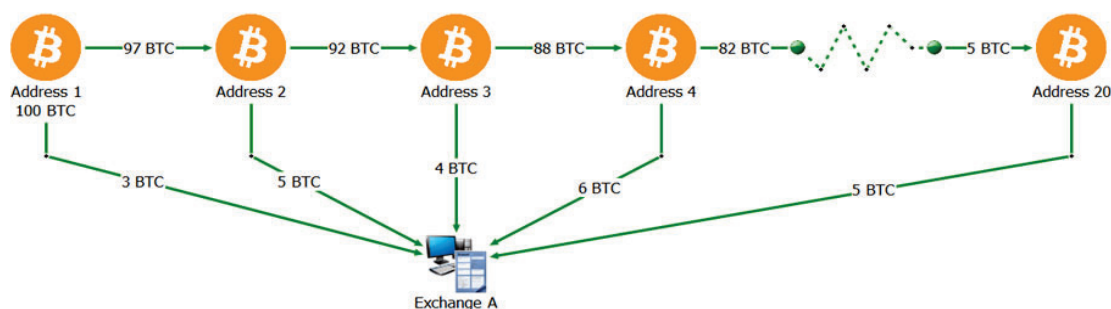
Thereafter, the funds were transferred through a series of intermediary addresses before beginning a “peel chain” of funds to the BINANCE ACCOUNTS as summarized in the chart below.

25. Based on my training and experience investigating digital currency transactions, I know that the term “peel chain” is used to describe a series of linked financial transactions involving cryptocurrency. A “peel chain” occurs when a large amount of cryptocurrency, like bitcoin, which is held on deposit at one address is sent to other addresses in a series of successive transactions. With each transaction down the line or “chain,” decreasing amounts of bitcoin are transferred from one address to the next. Residual amounts associated with each transaction are “peeled off” the chain to an additional address (frequently, to be deposited into a virtual currency exchange). In my training and experience, I know that it is common for money launderers to

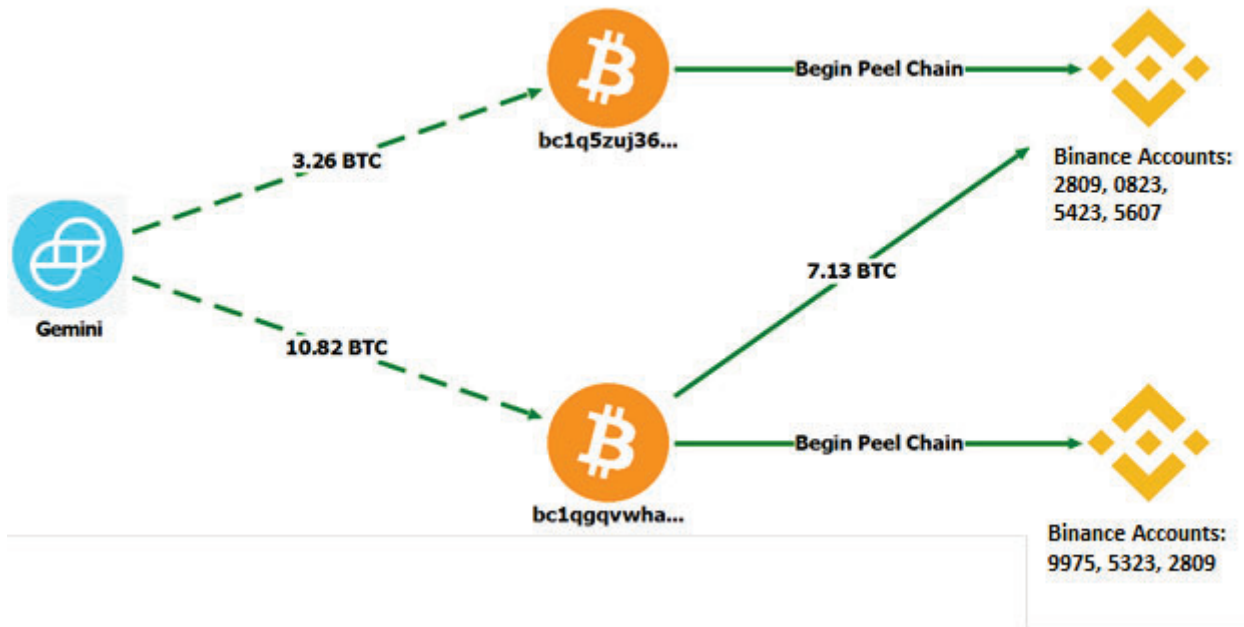
⁸Records obtained from Gemini reflect corresponding deposits totaling \$898,342 to Gemini Account 1 on or about the same dates.

rely on a peel chain to obstruct the movement of illicit money.

26. The chart below illustrates a simple peel chain example where a hypothetical person, seeking to deposit 100 BTC into a virtual currency exchange, uses the peel chain technique to make the transactions difficult to trace. From left to right, the person(s) forwards a total of 100 BTC through a series of transactions with 20 peels in inconsistent amounts, ultimately depositing the final five BTC into the virtual currency exchange, at which point all 100 BTC have been deposited.



27. As noted above, based on my review of the blockchain in this investigation, the \$898,342 was withdrawn into three different BTC addresses, subsequently collated into two different addresses and finally moved from those two addresses through a peel chain of funds into the BINANCE ACCOUNTS below:



28. The movement of these funds into the BINANCE ACCOUNTS are consistent with tactics typically employed in money laundering transactions, used for the purpose of attempting to conceal the origin of the fraud proceeds. In this case, the fraudsters obfuscated linear lines of blockchain transactions, separated victim proceeds, and co-mingled the victim's funds with other funds of unknown origin. Further, the number of "hops" in these transactions appear to lack any ostensible business purpose and further establish probable cause to believe that the transfers were coordinated and intended to obscure the control, ownership, source, and purpose of the funds involved in said transfers.

29. BINANCE ACCOUNT 0976 – According to blockchain analysis and records from Binance, on or about March 21, 2022, BINANCE ACCOUNT 0976 received approximately 0.0068488 BTC of stolen funds. According to records from Binance, the account had a balance of approximately 0.56703459 BTC on or about May 17, 2022. Pursuant to a

seizure warrant for things of value up to 0.0066488 BTC in BINANCE ACCOUNT 0976, 0.0066488 BTC was seized on or about August 22, 2022.

30. BINANCE ACCOUNT 0823 – According to blockchain analysis and records from Binance, on or about March 21, 2022, BINANCE ACCOUNT 0823 received approximately 0.02446 BTC of stolen funds. According to records from Binance, the user of the account then converted the funds to Tether, also known as USDT. Based on my training and experience, the user of the account then sells USDT via Binance’s peer-to-peer trading platform.⁹ Pursuant to a seizure warrant for things of value up to 0.02426 BTC from BINANCE ACCOUNT 0823, 0.02426 BTC was seized on or about August 22, 2022.

31. BINANCE ACCOUNT 5423 – According to blockchain analysis and records from Binance, on or about March 18, 2022, BINANCE ACCOUNT 5423 received approximately 0.02476 BTC of stolen funds. According to records from Binance, the user of the account converted the funds to USDT. Pursuant to a seizure warrant for things of value up to 0.02476 BTC in BINANCE ACCOUNT 5423, 736.652108 USDT was seized on or about August 23, 2022.

32. BINANCE ACCOUNT 5607 – According to blockchain analysis and records from Binance, on or about March 22, 2022, BINANCE ACCOUNT 5607 received approximately 1.4568 BTC of stolen funds. According to records from Binance, the user of the account converted the funds to USDT and withdrew them. The account had a balance of approximately 0.20146528 BTC equivalent on or about April 04, 2022. Pursuant to a seizure warrant for things of value up to 1.4568 BTC in BINANCE ACCOUNT 5607, 19512.815843

⁹ Binance users may send, receive, and trade numerous different virtual currency assets. These assets may include BTC, USDT, and other coins/tokens. Binance provides a BTC equivalent value for all assets held within an account.

USDT, 27.58652 APE, 10292.6775 JASMY, 648.193 OGN, and 18906045.54 SHIB were seized on or about August 23, 2022 and 5113150.55 XEC was seized on or about September 19, 2022.

33. BINANCE ACCOUNT 9975 – According to blockchain analysis and records from Binance, between approximately March 16, 2022 and March 18, 2022, BINANCE ACCOUNT 9975 received approximately 2.27188039 BTC of stolen funds via several transactions. According to records from Binance, these funds were converted to USDT and withdrawn. BINANCE ACCOUNT 9975 had a BTC equivalent balance of approximately 0.0567562 BTC on or about April 04, 2022. Pursuant to a seizure warrant for things of value up to 1.4568 BTC in BINANCE ACCOUNT 9975, 1577.9271 USDT and 19240.7898 TLM was seized on or about August 23, 2022.

34. BINANCE ACCOUNT 5323 – According to blockchain analysis and records from Binance, between approximately March 16, 2022 and March 17, 2022, BINANCE ACCOUNT 5323 received several deposits of stolen funds totaling approximately 1.63930574 BTC. According to records from Binance, these funds were converted to USDT. The majority of funds associated with BINANCE ACCOUNT 5323 were converted to USDT and sold via Binance's peer-to-peer platform for Nigerian Naira. BINANCE ACCOUNT 5323 had a balance of approximately 0.011585575 BTC equivalent on or about April 04, 2022. Pursuant to a seizure warrant for things of value up to a value of 1.63930574 BTC in BINANCE ACCOUNT 5323, 0.00217033 BTC and .01266977 BNB was seized on or about August 22, 2022.


35. BINANCE ACCOUNT 2809 – According to blockchain analysis and records from Binance, on or about March 16, 2022, BINANCE ACCOUNT 2809 received approximately 0.09765498 BTC of stolen funds. According to records from Binance, these funds were converted to USDT. Based on my training and experience and review of Binance

account records, the account was primarily used to convert funds to USDT and sell those funds for Naira via Binance's peer-to-peer platform. BINANCE ACCOUNT 2809 had a balance of approximately 0.010926432 BTC equivalent on or about April 04, 2022. Pursuant to a seizure warrant for things of value up to a value of 0.09765498 BTC in BINANCE ACCOUNT 2809, 2875.828369 USDT was seized on or about August 23, 2022.

CONCLUSION

36. Based on the foregoing, as well as my training, education, and experience, there is probable cause to believe that Defendant Cryptocurrency is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

Pursuant to 28 U.S.C. § 1746, I declare under the penalties of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 22 day of May, 2023.



Special Agent Brian Pereira,
Federal Bureau of Investigation